UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/073,017	02/12/2002	Mikio Torii	1247-0473P	3093

2292 7590 12/20/2006
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
BAUM, RONALD	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/20/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/073,017	**Applicant(s)** TORII ET AL.	
	Examiner Ronald Baum	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *9/22/06*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 24 August 2006.

2. Claims 1, 3-12 are pending for examination.

3. Claims 1, 3-12 remain rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 3-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Shanton, U.S. Patent 5,680,452.

4. As per claim 1; "An encryption processing apparatus comprising:

necessity determination means for

determining whether or not received data needs to be encrypted *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (i.e., col. 4,lines 38-65, video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated storage forms (i.e., col. 4,lines 38-65, the hard drive, RAM, CD, queues, network memory elements, printer buffers, etc.) that are further selectively determined to be encrypted (i.e., col. 3,lines 53-65, col. 4,lines 5-38, upon receipt of the data to the encrypting system/device), both in a serial object manor, or in* *an encapsulated/inheritance object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*;

encryption means for

encrypting data which is determined as having to be encrypted, before being stored in a storage apparatus to output *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the objects (data) that are determined to be encrypted (i.e., col. 3,lines 53-65, col. 4,lines 5-38), residing in the associated storage forms for which the host processing element will perform the pre-selected form of encryption upon, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*; and

storage form determination means for

determining a storage form of the storage apparatus,

wherein the necessity determination means

determines whether or not the data needs to be encrypted, based on

a determination result of the storage form determination means,

and

wherein the necessity determination means

determines whether or not to encrypt the received data based on

whether the storage form determination means determines that

the storage form is

volatile or

non-volatile *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the received objects defined across all types of*

> *data forms and associated storage forms (i.e., col. 3,lines 52-col. 4,lines 65, such that properly specified kinds of information flowing to appropriate locations; 'kinds' encompasses multimedia (non-volatile DVD/CD or volatile resident RAM when being processed) storage forms) that are further selectively determined to be encrypted, both in a serial object manor, or in an encapsulated/inheritance/access controlled object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*".

5. Claim 3 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 1, wherein

in cases where the storage form determination means determined the received data as being to be maintained in the storage apparatus even when the storage apparatus is <u>removed</u>,

the necessity determination means determines that the data needs to be encrypted.".

The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the received objects defined across all types of data forms and associated storage forms, (i.e., col. 3,lines 52-col. 4,lines 65, such that properly specified kinds of information flowing to appropriate locations; 'kinds' encompasses multimedia (non-volatile DVD/CD or volatile resident RAM when being processed) storage forms) especially as is concerned with network element/object to network element/object transfer/controlled access, that are further selectively pre-determined to be encrypted prior to transfer/storage across the network, both in a serial object manor, or in an encapsulated/inheritance/access controlled object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

6. Claim 4 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 1, wherein

the necessity determination means is constructed so as to

determine whether or not the data needs to be encrypted based on

a form or

items of the data.".

The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (and data item components, i.e., video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated transfer/storage protocols (utilized in said transfer/storage) that are further selectively determined to be encrypted; therefore inherently possess a form (i.e., the various flags and status bytes inherent to said protocols that determine the transfer routing/addressing/access rights/etc.,), as appended to the data/data content object structures/streams so transferred, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

7. Claim 5 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 4, wherein

in cases where the received data is presented in an encrypted form,

the necessity determination means

determines that the received data does not need to be encrypted.".

The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (and data item components) and associated transfer/storage protocols (utilized in said transfer/storage) that are further selectively determined to be encrypted and as such are subsequently encrypted; clearly are not re-encrypted and therefore, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

8. Claim 6 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 4, wherein

in cases where an item of the received data is an indicator regarding importance of data,

the necessity determination means

determines that the received data needs to be encrypted.".

The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (and data item components, i.e., video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated transfer/storage protocols (utilized in said transfer/storage) that are further selectively determined to be encrypted; therefore inherently possess a form (i.e., the various flags and status bytes inherent to said protocols that determine the transfer routing/addressing/access rights/etc.,), as appended to the data/data content object structures/streams so transferred, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

9. Claim 7 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 6, wherein

the indicator is

a flag or

an instruction for confidential.".

The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (and data item components, i.e., video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated transfer/storage protocols (utilized in said transfer/storage) that are further selectively determined to be encrypted upon request or instruction; therefore inherently possess a form (i.e., the various flags and status bytes inherent to said protocols that determine the transfer routing/addressing/access rights/encryption parameters (i.e., confidential or so related levels of security aspects) and specificity, etc.,), as appended to the data/data content object structures/streams so transferred, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

10. Claim 8 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 4, wherein

in cases where an item of the received data is a predetermined condition, the necessity determination means

determines that the received data needs to be encrypted.".

The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (and data item components, i.e., video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated transfer/storage protocols (utilized in said transfer/storage) that are further selectively determined to be encrypted; therefore inherently possess a form (i.e., the various flags and status bytes inherent to said protocols that determine the transfer routing/addressing/access rights/etc.,), as appended to the data/data content object structures/streams so transferred, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

11. Claim 9 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 1, further comprising:

decryption means for decrypting the encrypted data which is stored in the storage apparatus,

wherein the data is outputted after being decrypted by the decryption means.".

The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the objects (data) that are determined to be encrypted, residing in the associated storage forms for which the host processing element will perform the pre-selected form of encryption upon, clearly will be subsequently decrypted upon determination of both valid use request or retrieved form determination so associated with the request, and therefore clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

12. Claim 10 ***additionally recites*** the limitation that; "The encryption processing apparatus of claim 1,

the encryption processing apparatus being used as an apparatus at a data receiving side.". The teachings of Shanton suggest such limitations (Abstract, col. 3,lines 51-col. 14,line 40, whereas the objects (data) that are determined to be encrypted, residing in the associated storage forms for which the host processing element will perform the pre-selected form of encryption upon, clearly will be subsequently decrypted upon determination of both valid use request or retrieved form determination so associated with the request, and therefore clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

13. As per claim 11; "An encryption processing system comprising:

a host apparatus for offering services such as data creation *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (i.e., col. 4,lines 38-65, video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated object creation/applications performing the object instantiation (i.e., host and network client/server word processing, image processing/rendering, etc.,), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*; and

an encryption processing apparatus which

encrypts data received from the host apparatus,

stores the encrypted data in the storage apparatus, and outputs the data from the storage apparatus *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (i.e., col. 4,lines 38-65, video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated object creation/applications performing the object instantiation (i.e., host and network client/server word processing, image processing/rendering, etc.,) and storage forms (i.e., the hard drive, RAM, CD, queues, network memory elements, printer buffers, etc.) that are further selectively determined to be encrypted (i.e., col. 3,lines 53-65, col. 4,lines 5-38, upon receipt of the data to the encrypting system/device), both in a serial object manor, or in an encapsulated/inheritance object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*,

wherein the host apparatus is provided with condition providing means for

providing a condition concerning encryption to data created by the host apparatus before transmitting to the encryption processing apparatus *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (and data item components, i.e., col. 4,lines 38-65, video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated transfer/storage protocols (utilized in said transfer/storage) that are further selectively determined to be encrypted; therefore inherently possess a form (i.e., the various flags and status bytes inherent to said protocols that determine the transfer routing/addressing/access rights/etc.,), as appended to the data/data content object structures/streams so transferred, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]* and

wherein the encryption processing apparatus comprises necessity determination means for

determining based on presence or absence of the condition,

whether or not received data needs to be encrypted *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (i.e., col. 4,lines 38-65, video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated storage forms (i.e., the hard drive, RAM, CD, queues, network memory elements, printer buffers, etc.) that are further selectively determined to be encrypted (upon receipt of the data to the encrypting system/device), both in a serial object manor, or in an encapsulated/inheritance object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*; and

storage form determination means for

determining a storage form of the storage apparatus,

wherein the encryption processing apparatus

encrypts at the encryption processing apparatus side the received data when

the necessity determination means determines

that the received data needs to be encrypted, and

wherein the condition is

whether the storage form determination means determines that

the storage form is

volatile or

non-volatile *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the received objects defined across all types of data forms and associated storage forms (i.e., col. 3,lines 52-col. 4,lines 65, such that properly specified kinds of information flowing to appropriate locations; 'kinds' encompasses multimedia (non-volatile DVD/CD or volatile resident RAM when being processed) storage forms) that are further selectively determined to be encrypted, both in a serial object manor, or in an encapsulated/inheritance/access controlled object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*".

15. As per claim 12; "An encryption processing apparatus comprising:

necessity determination means for

determining whether or not received data needs to be encrypted *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the use of objects defined across all types of data (i.e., col. 4,lines 38-65, video, printer/printer buffer, sound, executable, general data formatted, etc.) and associated storage forms (i.e., col. 4,lines 38-65, the hard drive, RAM, CD, queues, network memory elements, printer buffers, etc.) that are further selectively determined to be encrypted (i.e., col. 3,lines 53-65, col. 4,lines 5-38, upon receipt of the data to the encrypting system/device), both in a serial object manor, or in* *an encapsulated/inheritance object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*;

encryption means for

encrypting data which is determined as having to be encrypted, before being stored in a storage apparatus to output *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the objects (data) that are determined to be encrypted (i.e., col. 3,lines 53-65, col. 4,lines 5-38), residing in the associated storage forms for which the host processing element will perform the pre-selected form of encryption upon, clearly encompasses the claimed limitations as broadly interpreted by the examiner.],*

wherein the encryption processing apparatus is an image forming apparatus *[Abstract, col. 3,lines 51-col. 14,line 40, whereas the received objects defined across all types of data forms and associated storage forms (i.e., col. 3,lines 52-col. 4,lines 65, such that properly specified kinds of information flowing to appropriate locations; 'kinds' encompasses multimedia (non-volatile DVD/CD or volatile resident RAM when being processed, or more generally when the multimedia/image data is formed in memory during said processing and associated encryption) storage forms) that are further selectively determined to be encrypted, both in a serial object manor, or in an encapsulated/inheritance/access controlled object data structure, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]*.".

Conclusion

16. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov . The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/03/06

Ronald Baum

Patent Examiner

Ronald Baum